รับมือ ไวรัส คอมพิวเตอร์

กองบรรณาธิการ

ในเรื่องของไวรัสคอมพิวเตอร์นั้น เราจะได้ยินข่าวทั้งในและนอกประเทศเกี่ยวกับการระบาดของมัน ซึ่งลักษณะการแพร่ของไวรัสแต่ละชนิดนั้น ก็ใช้เทคนิคที่ต่างกันไป โดยที่ไวรัสคอมพิวเตอร์ส่วนใหญ่ที่พบในบ้านเราจะมาจากต่างประเทศเกือบทั้งสิ้น นอกจากนี้อาจจะมีการปรับปรุงเสริมแต่งบ้าง ซึ่งจะสังเกตได้จากลักษณะของไวรัสที่มีโปรแกรมการทำงานคล้ายกันมาก ๆ

ไวรัสในบ้านเรา

ไวรัสที่พบในบ้านเราในเครื่อง PC มีหลายชนิดด้วยกัน ซึ่งจะเรียกชื่อต่าง ๆ กันตามลักษณะกลุ่มของชนิดดังนี้

- @ Brain หรือ (c) Brain หรือ Pakistani Brain

- Alameda หรือ FATERASER หรือ T-2 หรือ 1K

- Friday the 13th หรือ sUMsDos หรือ Israeli หรือ Hebrew หรือ Glue

- Lehigh/COMMAND.COM

- THE 3 WISE MEN หรือ Y.C.1.E.R.P

ซึ่งไวรัสที่พบมากในบ้านเราอยู่ในกลุ่มของ (c)Brain, T-2 และ sUMsDos

ทำอย่างไรดี

"การระวังรักษาสุขภาพของตนเองให้ดี จะทำให้ปราศจากโรคภัย" เช่นเดียวกัน ไวรัสคอมพิวเตอร์จะไม่สามารถระบาดเข้าไปในคอมพิวเตอร์ของคุณได้ ถ้าคุณมีการระวังป้องกันและเตรียมพร้อมที่จะรับมือกับมัน บทบัญญัติ 10 ประการง่าย ๆ ต่อไปนี้ จะเป็นการสร้างป้อมปราการที่สำคัญในการขวางกั้นไม่ให้เจ้าไวรัสเข้ามาในดินแดนของเรา

1. แบคอัพข้อมูลบ่อย ๆ ชุดเดียวไม่พอแน่ ควรมีหลาย ๆ ชุดที่จะหมุนเวียนกันไป เช่น ในหนึ่งสัปดาห์ควรมีดิสเกตต์ 7 ชุดในการแบคอัพในแต่ละวัน (อะไรจะมากมายขนาดนั้น) มันอาจจะเสียเวลาและยุ่งยากบ้าง แต่เมื่อวันใดที่เกิดติดไวรัสขึ้นมา แล้วมันเกิดทำลายข้อมูลของเรา ถึงตอนนั้นเราคงไม่ต้องมานั่งตาถลนเพื่อกู้ข้อมูลสำคัญที่เราได้สะสมไว้มาเป็นแรมเดือน (กันไว้ดีกว่าแก้)

2. ถ้ารู้แน่ว่าไวรัสเข้าไปทำลายข้อมูลและเข้าสู่ระบบในเครื่องคอมพิวเตอร์ของคุณแล้ว ไม่ต้องตกใจ (รีบหยิบยาดมขึ้นมา) ข้อมูลที่ถูกทำลายไปอาจเพียงเล็กน้อย คุณยังสามารถกู้สถานการณ์ได้ โดยการปิดเครื่องแล้วบูตด้วยดอสที่คุณแน่ใจว่าไม่มีไวรัสแน่นอน (ควรเป็น Original disks) จากนั้นฟอร์แมตฮาร์ดดิสก์โดยใช้คำสั่ง FORMAT.COM และใช้คำสั่ง RESTORE

โดยเลือกเฉพาะดาต้าไฟล์จากแบคอัพของคุณเท่านั้น แล้วย้ายโปรแกรมไฟล์กลับคืนสู่ฮาร์ดดิสก์ของคุณ ซึ่งควรจะใช้ Original disks เช่นกัน (โล่งอกไปที)

3. แปะ write-protect บนแผ่นดิสเกตต์ทุกแผ่นที่ไม่ได้ใช้สำหรับเขียนข้อมูลลงไป (เปลืองน่าดู) แล้วถ้าอยู่ดี ๆ คุณรันโปรแกรมแล้วเจ้าไวรัสพยายามจะเขียนตัวมันเองลงบนแผ่นที่ติด write-protect ละก็ จะปรากฏข้อความแจ้ง error ที่พยายามเขียนดิสค์ทันที แค่นี้ก็พอจับได้แล้วว่ามันกำลังจะประพฤติมิดีมิร้ายกับแผ่นดิสค์ของเรา (ตาวิเศษเห็นนะ)

4. อย่าไว้ใจทาง อย่าวางใจ bulletin board อย่าเพิ่งไว้ใจ ซอฟต์แวร์ที่มาจาก bulletin board รอสักระยะหนึ่งก่อน อย่าเพิ่งใช้ให้สังเกตบันทึกจาก BBSs ที่เช็คโดย sysop ก่อน ถ้าโปรแกรมมาจากผู้เขียนโดยตรงและมีชื่อหรือ document file กำกับ ก็พอจะวางใจได้ แต่ทางที่ดีให้รออีกสัก 2-3 อาทิตย์ เพื่อดูว่าโปรแกรมนี้สร้างปัญหาให้กับคนอื่น ๆ หรือไม่ ถ้าไม่ก่อความเดือดร้อนใด ๆ ก็ลงมติไว้วางใจได้ (ผ่านเข้าสภาของเราได้เลย)

5. เปลี่ยนแอตทริบิวต์ของไฟล์ .COM และ .EXE ให้อ่านได้อย่างเดียว ถ้ามีดอสเวอร์ชัน 3.3 จะทำได้ง่ายมาก โดยใช้โปรแกรม ATTRIB จากไดเรคทอรีราก แล้วใช้คำสั่ง

ATTRIB +R *.COM /S

(/S นั้นเป็นสวิตช์บอกให้เอกซีคิวต์คำสั่งทุกสับไดเรคทอรี) จากนั้นใช้คำสั่งเดิมอีกครั้ง แต่เปลี่ยน *.COM เป็น *.EXE แค่นี้ก็เรียบร้อยแล้ว เดี๋ยวก่อน...ถ้าเกิดไม่มีดอส 3.3 จะทำอย่างไรดี ก็ใช้ PCTOOLS ไง (อย่าบอกนะว่าไม่มีอีก เชยจริง ๆ)

6. ย้ายบ้านหนีกันเลย โดยย้าย COMMAND.COM ในฮาร์ดดิสค์จากไดเรคทอรีรากไปไว้สับไดเรคทอรีอื่นซะ เช่นย้ายไปไว้ในสับไดเรคทอรี HIDDEN ที่ได้สร้างไว้แล้ว

จากนั้นในไฟล์ CONFIG.SYS ของคุณให้เพิ่มบรรทัดดังนี้

SHELL = C:\HIDDEN\COMMAND.COM /P

แล้วเพิ่มบรรทัดดังต่อไปนี้ในไฟล์ AUTOEXEC.BAT คือ

SET COMSPEC=C:\HIDDEN\COMMAND.COM

เอาล่ะเรียบร้อย ถ้ายังขยันที่จะซ่อนไฟล์อีกละก็ ซ่อนมันทั้ง COMMAMD .COM และไดเรคทอรี HIDDEN ด้วยก็ได้ โดยใช้โปรแกรม ATTR.COM (หาเอาเอง)

7. หวงดิสค์ไว้ อย่าให้ใครยืมเด็ดขาด เพราะมันอาจติดโรคไวรัสกลับมาก็ได้ แต่ถ้าแฟนมายืม (ไม่เป็นไร) ให้ DISKCOPY อีกแผ่นหนึ่งให้เธอไป แล้ววันหลังเมื่อเธอเอามาคืน ก็ให้ฟอร์แมตแผ่นนั้นใหม่เสีย ถ้ากรณีเธอจะยืมฮาร์ดดิสค์ ก็ซื้อให้ใหม่เสียเลย (ยินดีไม่มีปัญหา)

8. ถ้าคุณยากจนไม่มีฮาร์ดดิสค์ การบูตซิสเต็มให้บูตเฉพาะแผ่นบูตจากดิสเกตต์แผ่นใดแผ่นหนึ่งเท่านั้น ไม่ควรมีแผ่นบูตหลาย ๆ แผ่น แล้วแปะ write-protect ไว้ด้วยอย่าลืม ในกรณีของผู้มี

ฮาร์ดดิสค์ ก็ให้บูตซิสเต็ม จากฮาร์ดดิสค์เท่านั้น (อย่าหลายใจเชียวนะ)

9. อย่าให้ใครก็ตามใช้เครื่องของคุณ (จะหวงไปถึงไหน) ถ้าเป็นเพื่อนสุดรัก ก็ให้ใช้เฉพาะโปรแกรมของเราเท่านั้น ห้ามใช้โปรแกรมที่เค้านำมาด้วย (มีแค่ไหนเล่นแค่นั้นก็พอ)

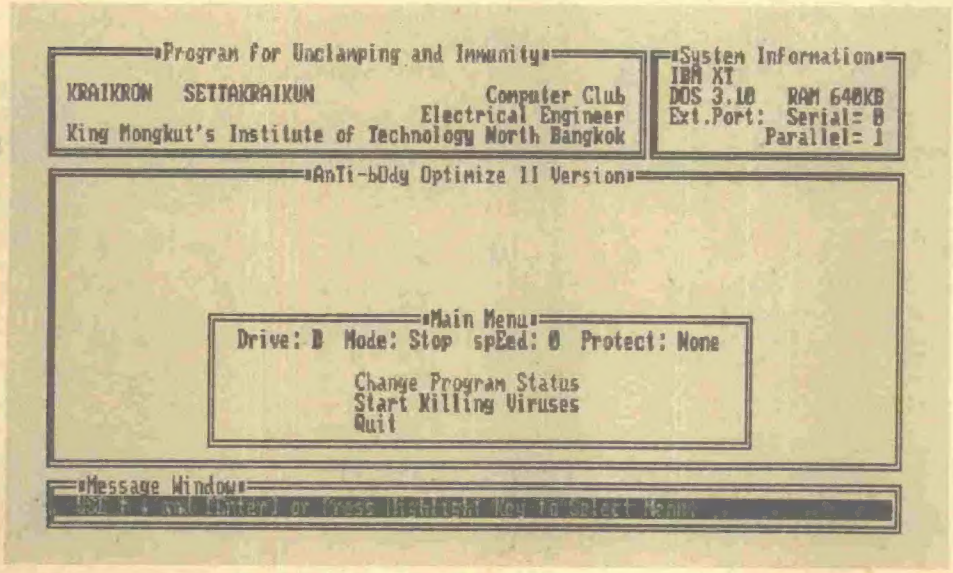
10. อย่าใช้โปรแกรมที่ได้มาจากก๊อบปี้ โดยไม่ถูกต้อง (อดไม่ได้จริง ๆ) เคยมีตัวอย่างมาแล้ว คือ โปรแกรมเกมตัวหนึ่ง ที่ได้ก๊อบปี้โดยการถอดก๊อบปี้โปรเท็คออกแล้ว ทำให้เกิดมีโค้ดทำลายโปรแกรมขึ้น ซึ่งจะออกฤทธิ์เมื่อเราเล่นเกมจนชนะ (ไม่ Happy ending เหมือนในหนังหรอกนะ)

จากบทบัญญัติ 10 ประการในการปฏิบัติตนนั้นก็พอจะช่วยให้คุณแคล้วคลาดจากโรคภัยไวรัสคอมพิวเตอร์ได้ ซึ่งถ้าคุณปฏิบัติครบ 10 ข้ออย่างเคร่งครัดแล้ว คิดว่าโอกาสที่จะติดไวรัสนั้น แทบจะเป็น 0% แต่ถ้าดวงไม่ดีเกิดติดขึ้นมาอีกละก็ ไม่เป็นไร มาตรการต่อไป คือ การกำจัดให้สิ้นซาก ถอนรากถอนโคนกันไปเลยทีเดียว ซึ่งก็ต้องยกให้เป็นหน้าที่ของโปรแกรมปราบไวรัสคอมพิวเตอร์ ซึ่งในบ้านเรานั้นมีโปรแกรมปราบไวรัสหลายตัวทีเดียว จะยกตัวอย่างให้ดูคุณสมบัติบางตัวดังนี้

ANTI.COM

ผลงานของคุณไกรกร เศรษฐไกรกุล เป็นเวอร์ชันที่ได้แก้ไขข้อบกพร่องต่าง ๆ ในเวอร์ชันก่อน ๆ และปรับปรุงการใช้ให้ง่ายขึ้นโดยใช้ลักษณะของเมนูคำสั่งเข้าช่วย

สามารถตรวจจับไวรัสได้ 6 ชนิด ซึ่งเป็นกลุ่มของไวรัสที่มีอยู่ในบ้านเราขณะนี้การทำงานของโปรแกรมนั้นสามารถสแกนหาไวรัสในไดเรคทอรีย่อยที่มีอยู่ทั้งหมดได้ พร้อมทั้งยังสามารถปรับความเร็วของโปรแกรมได้ ทั้งนี้เพื่อความสะดวกในการดูชื่อไฟล์ต่าง ๆ ที่กำลังตรวจจับไวรัสอยู่



รูปที่ 1 หน้าตาของ ANTI.COM

การกำจัดไวรัสในหน่วยความจำนั้น ถ้าเป็นไวรัสประเภทบูตเซกเตอร์ จะทำการรีเซตเครื่องให้ใหม่ แต่ถ้าเป็นไฟล์ไวรัสจะจัดการกำจัดในหน่วยความจำได้เลย โดยไม่ต้องรีเซตเครื่องใหม่ หน้าตาของโปรแกรม ดังรูปที่ 1

RTAF1.COM

โปรแกรมที่กำจัดไวรัส sUMsDos โดยเฉพาะ ผู้เขียนคือคุณสานนท์ แก้วอบเชย ผู้ใช้เพียงแต่ใส่ชื่อไดรฟ์หรือสับไดเรคทอรีที่ต้องการตรวจสอบเท่านั้น ในกรณีที่มีไวรัสนี้ในซิสเต็มของเราอยู่ก่อนแล้ว จะให้ทำการรีบูตใหม่ ลักษณะทั่วไปของการใช้งานไม่ค่อยสะดวกนัก ถ้ามีสับไดเรคทอรีมาก เนื่องจากโปรแกรมไม่เข้าไปในสับไดเรคทอรีต่าง ๆ ให้เราต้องบอกให้โปรแกรมทราบเอง

PURE22.EXE

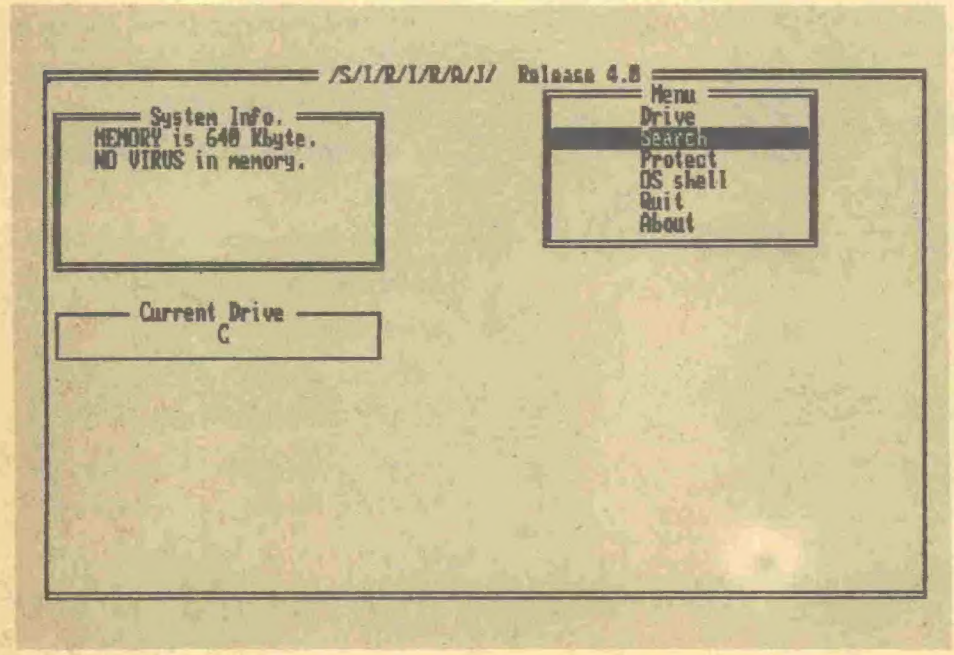
ผลงานของ EGAT เรานี่เองเขียนโดยคุณอนุชิต จารุจุมพล ซึ่งเป็นรีลิสต์ 2.2 (พัฒนามาจาก PURE2) การทำงานของโปรแกรมจะเป็นรายการให้เลือก โดยสามารถออกจากโปรแกรม หรือเบรคการทำงานของโปรแกรมขณะตรวจเช็ค นอกจากนี้ยังสามารถเลือกไดรฟ์ได้ ลักษณะของโปรแกรมนั้นจะสามารถเลือกการตรวจสอบได้อย่างเดียว หรือตรวจสอบกำจัดเลยก็ได้ ใช้ได้กับไวรัส sUMsDos เท่านั้น โดยเมื่อเรียกโปรแกรมจะทำการตรวจเช็คไวรัสในหน่วยความจำให้เลย เมื่อพบจะรายงานให้ทราบแต่ไม่กำจัดให้ ซึ่งเราสามารถใช้โปรแกรม FREEZE2.EXE ซึ่งมาคู่กันกับ PURE22.EXE นี้ในการป้องกันไม่ให้ไวรัสที่เข้าไปอยู่ในซิสเต็มทำงานได้ (ถึงแม้มันจะยังอยู่ก็ตาม) ส่วนการทำงานของโปรแกรมนั้น ค่อนข้างรวดเร็วมาก โดยจะสแกนหาในทุกสับไดเรคทอรีที่มีให้โดยอัตโนมัติ พร้อมทั้งรายงานไฟล์ที่พบไวรัสด้วย

SIRIRAJ4.EXE

ล่าสุดจากการพัฒนาโปรแกรม SIRIRAJ ของคุณสุรเมธ สัจจอิสริยวุฒิ ที่เรารู้จักกันดี ซึ่งเป็นรีลิส 4.0 สามารถตรวจสอบและรักษาครอบคลุมไวรัสที่มีทั้งหมดในบ้านเราขณะนี้ ลักษณะหน้าตาเป็นเมนูวินโดว์ให้เลือกคำสั่งดังรูปที่ 2 โดยใช้คีย์ลูกศรทำให้ใช้งานได้ง่ายมาก

ไวรัสที่อยู่ในหน่วยความจำนั้น โปรแกรมสามารถตรวจเช็ค และกำจัดได้ ยกเว้นไวรัส sUMsDos ซึ่งจะต้องใช้โปรแกรม SIRIRAJV ควบคู่ในการป้องกันการทำงานของไวรัสนี้ในหน่วยความจำ ส่วนการรักษาไวรัสในแผ่นดิสค์นั้น พบจุดอ่อนเล็กน้อยในเรื่องที่เกิดจากการปิด write-protect คือ ถ้าในแผ่นดิสค์ที่มีไวรัส (ในบูตเซกเตอร์) คือ (c) Brain หรือ T-2 แล้วปิด write-protect ไว้ เมื่อตรวจพบไวรัสโปรแกรมจะไม่เตือนให้แกะ write-protect ออก จะดำเนินการรักษาทันที และรายงานว่าดิสค์ปราศจากไวรัสแล้ว ซึ่งที่จริงนั้นไวรัสยังอยู่ในบูตเซกเตอร์นี้ ดังนั้นจึงควรที่จะแกะ write-protect ของแผ่นที่ต้องการตรวจไวรัสออกก่อน ส่วนลักษณะเดียวกันในกรณีของไวรัส sUMsDos นั้น ไม่เกิดปัญหาดังกล่าว

ตัวอย่างโปรแกรมกำจัดไวรัสเหล่านี้ได้รวบรวมไว้ในซอฟต์เมล์ฉบับนี้ รวมทั้งโปรแกรม VIRUSLAB และ FRIDAY ซึ่งได้เคยลงในไมโครฯ 47 และ 50 แล้วตามลำดับ ซึ่งโปรแกรม VIRUSLAB นั้น ใช้สำหรับไวรัสประเภทบูตเซ็กเตอร์ไวรัส ส่วนโปรแกรม FRIDAY นั้น ใช้สำหรับไวรัสประเภทไฟล์ไวรัส



รูปที่ 2 หน้าตาของ SIRIRAJ4.EXE

สรุป

ในขณะที่ไวรัสคอมพิวเตอร์กำลังระบาดอยู่นี้ โปรแกรมกำจัดไวรัสต่าง ๆ ก็ทยอยกันออกมาเรื่อย ๆ ซึ่งเพียงพอกับชนิดของไวรัสที่มีอยู่ในบ้านเรา โดยที่ทางฝ่ายกลุ่มผู้คิดค้นโปรแกรมแก้ไวรัสเหล่านี้ ก็ได้คิดค้นแก้ไขปรับปรุงโปรแกรมของตนอย่างต่อเนื่อง ซึ่งความสามารถของโปรแกรมเหล่านั้นก็ใช้ได้ดีพอสมควร และสามารถแก้ปัญหาการติดต่อได้โดยไม่ให้เกิดความเสียหายมากขึ้น ในปัจจุบันภาวะการระบาดของไวรัสในบ้านเราขณะนี้จึงไม่ควรวิตกให้มากนัก

ส่วนแนวโน้มการระบาดของไวรัสคอมพิวเตอร์ในอนาคตนั้น เป็นที่แน่นอนว่าจะต้องมีไวรัสชนิดใหม่ ๆ เกิดเพิ่มมากขึ้น ซึ่งจะสังเกตุได้จากในอดีตนั้นเริ่มจากการที่เราพบไวรัส (c) Brain เพียงชนิดเดียว ต่อจากนั้นก็มีไวรัสชนิดอื่นเกิดขึ้นตามมา โดยที่ในระยะแรกของการระบาดนั้น อาจจะไม่มีโปรแกรมที่จะมากำจัด ซึ่งจะส่งผลให้เกิดความเสียหายบ้าง แต่ในที่สุดก็มีอัศวินม้าขาวมาช่วยได้ทันท่วงทีทุกครั้งไป โปรแกรมที่กำจัดไวรัสในบ้านเราส่วนใหญ่ก็คิดโดยคนไทยเรานี้เอง

ดังนั้นสิ่งที่จะช่วยเราได้ในขั้นต้นนั้นก็คือ การระวังและป้องกันด้วยตนเองก่อน ซึ่งเป็นด่านสำคัญที่จะกันไม่ให้ไวรัสคอมพิวเตอร์เข้าสู่ระบบของเราได้ และถ้าทุกคนช่วยกันปฏิบัติแล้วละก็ การระบาดของไวรัสก็จะค่อย ๆ ลดน้อยลง และจะไม่เป็นเรื่องที่น่าวิตกอีก ผู้ที่คิดจะสร้างไวรัสขึ้นก็คงจะหันไปสร้างสรรค์ผลงานอย่างอื่น ที่ไม่ใช่เป็นการทำลาย หรือก่อความเดือดร้อนให้กับสังคมต่อไป